Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method of confirming proper receipt of e-mail, said method comprising the steps of:

obtaining an e-mail file which is intended by a sending party for transmission to a target e-mail address associated with a target party;

electronically transmitting the e-mail file from a ~~first~~ computer associated with the sending party and connected to a communications network;

delivering the e-mail file to a recipient e-mail address ~~which is~~ associated with a recipient ~~second~~ computer connected to the communications network;

detecting an access event generally associated with e-mail retrieval from the recipient e-mail address;

upon a detection of the access event executing the steps of:

discovering recipient data associated with the recipient e-mail address,

generating a confirmation of receipt notice containing the discovered recipient data, and

electronically transmitting the confirmation of receipt notice to a return e-mail address associated with the sending party for allowing a comparison of the discovered recipient data contained in the confirmation of receipt notice with intended delivery information associated with the target party in order to determine whether the e-mail file was delivered to the intended recipient.

2. (Currently amended) The method as in claim 1,

wherein the discovering step includes retrieving from a ~~the second~~ computer associated with the recipient party a pre-recorded ~~recipient~~ data file containing pre-recorded recipient data.

3. (Currently amended) The method as in claim 1,

further comprising the step of: obtaining recipient ~~accessing~~ party identity information from the recipient ~~accessing~~ party as a requisite condition for permitting access to the recipient e-mail address, and

wherein the discovering step includes retrieving the recipient ~~accessing~~ party identity information, and wherein the generating step includes such recipient ~~accessing~~ party identity information within the ~~recipient~~ data contained in the confirmation of receipt notice.

4. (Currently amended) The method as in claim 1,

further comprising the steps of: obtaining recipient ~~accessing~~ party identity information from the recipient ~~accessing~~ party as a requisite condition for operating a computer, said computer being operable by the recipient ~~accessing~~ party to gain access to the recipient e-mail address, and

wherein the discovering step includes retrieving the recipient ~~accessing~~ party identity information.

5. (Currently amended) The method as in claim 1,

wherein the discovering step includes electronically tapping a remote connection between the recipient ~~second~~ computer and a remote user computer operable by the recipient ~~accessing~~ party to gain remote access to the recipient e-mail address.

6. (Original) The method as in claim 1,

further comprising the step of:

transmitting and delivering to the recipient e-mail address an executable attachment file in conjunction with the e-mail file, the executable attachment file having a first module for discovering the recipient data, a second module for generating the confirmation of receipt notice, and a third module for electronically transmitting the confirmation of receipt notice,

and upon the detection of the designated access event, automatically executing the first, second, and third modules of the executable attachment file.

7. (Previously amended) The method as in claim 6,

wherein the executable attachment file has a fourth module transmitted and delivered therewith, the fourth module for detecting the designated access event, and

further comprising the step of:

automatically executing the fourth module upon delivery of the attachment file to the recipient e-mail address.

8. (Original) The method as in claim 1,

further comprising the step of determining, upon delivery of the e-mail file to the recipient e-mail address, whether the delivered e-mail file is of at least one designated file-type requiring a confirmation of receipt notice, and

wherein the detecting step occurs upon a determination that the delivered e-mail file is of the at least one designated file-type.

9. Canceled.

10. Canceled.

11. Canceled.

12. Canceled.

13. Canceled.

14. Canceled.

15. Canceled.

16. Canceled.

17. (Currently amended) A system for confirming proper receipt of e-mail transmitted over a communications network, said system comprising:

an e-mail file which is intended by a sending party for electronic transmission to

a target e-mail address associated with a target party;

a ~~first~~ computer associated with the sending party connected to the communications network and from which the sending party may electronically transmit the e-mail file;

a recipient computer connected to the communications network, the recipient computer having a data storage location for storably receiving the e-mail file;

first executable software means for detecting a designated access event generally associated with e-mail retrieval from the recipient e-mail address;

second executable software means for discovering recipient data associated with the recipient e-mail address;

third executable software means for generating a confirmation of receipt notice containing the discovered recipient data; and

fourth executable software means for electronically transmitting the confirmation of receipt notice ~~from the second computer~~ to a return e-mail address associated with the sending party,

wherein the second, third, and fourth executable software means are configured for automatic execution upon detection of the designated access event by the first executable software means,

whereby data contained in the confirmation of receipt notice may be compared to the delivery information associated with the target party to determine whether the e-mail file was delivered to the intended recipient.

18. (Currently amended) The system as in claim 17,

further comprising a pre-recorded ~~recipient~~ data file resident in a computer associated with the recipient ~~computer~~ party and containing the recipient data, and

wherein the second executable software means for discovering operates to retrieve the pre-recorded recipient data file from the recipient computer.

19. (Currently amended) The system as in claim 17,

further comprising a remote user computer which is remotely connected to the recipient computer and from which the recipient ~~accessing~~ party may gain remote access to the recipient e-mail address.

20. (Currently amended) The system as in claim 17,

further comprising recipient ~~accessing~~ party identifier means ~~resident on the recipient computer~~ for obtaining recipient ~~accessing~~ party identification information from the recipient ~~accessing~~ party as a requisite condition for permitting access to the recipient e-mail address; and

wherein the second executable software means for discovering recipient data operates to retrieve the recipient ~~accessing~~ party identification information.

21. (Currently amended) The system as in claim 17,

further comprising recipient ~~accessing~~ party identifier means for obtaining recipient ~~accessing~~ party identification information from the recipient ~~accessing~~ party as a requisite condition for operating a computer, and

wherein the second executable software means for discovering recipient data operates to retrieve the accessing party identification information.

22. (Previously amended) The system as in claim 19,

wherein the second executable software means for discovering recipient data operates to electronically tap the remote connection between the recipient computer and the remote user computer for obtaining remote access information associated with the remote connection.

23. (Previously amended) The system as in claim 17,

wherein the second, third, and fourth executable software means are third, fourth,

and fifth modules, respectively, of an executable attachment file transmitted and delivered in conjunction with the e-mail file.

24. (Original) The system as in claim 23,

wherein the first and second executable software means are first and second modules, respectively, of the executable attachment file, with said first module automatically executing upon delivery of the executable attachment file to the recipient e-mail address.

25. (Previously amended) The system as in clam 17,

further comprising a fifth executable software means for determining whether the delivered e-mail file is of at least one designated field-type requiring a confirmation of receipt notice, and

wherein the first executable software means is automatically executed upon a determination that the delivered e-mail file is of the at least one designated file-type requiring a confirmation of receipt notice.

26. (Previously presented) The system as in Claim 17, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

27. (Previously presented) The system as in Claim 17, wherein said recipient computer is a user system that is directly accessible by said recipient party, said user system including an electronic mail processing software and being capable of receiving e-mail.

28. (Currently amended) The system as in Claim 17, wherein the ~~third~~ second executable software means for discovering recipient data operates to electronically tap the remote connection between the computer associated with the sending party and the recipient computer for obtaining remote access information associated with the remote connection.

29. (Currently amended) The system as in Claim 19, wherein the ~~third~~ second executable software means operates to discover remote access information associated with the remote access of the recipient e-mail address from the remote user computer.

30. (Currently amended) The system as in Claim 20, wherein said recipient ~~accessing~~ party identification information is stored in the recipient computer.

31. (Previously presented) The system as in Claim 20, wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

32. (Currently amended) The system as in Claim 21, wherein said recipient ~~accessing~~ party identification information is stored in said computer.

33. (Previously presented) The system as in Claim 21, wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

34. (Previously presented) The system as in Claim 21, wherein said computer is the recipient computer.

35. (Previously presented) The system as in Claim 21, wherein said computer is a remote user computer.

36. (Previously presented) The system as in Claim 17, wherein said confirmation of receipt notice is used to verify proper delivery of legal documents.

37. (Previously presented) The system as in Claim 17, wherein said confirmation of receipt

notice is used to verify proper delivery of confidential documents.

38. (Currently amended) The system as in Claim 17, wherein said recipient data comprises, at least in part, identity information associated with said recipient ~~accessing~~ party.

39. (Previously presented) The system as in Claim 38, wherein said identity information pertains to biometric identification.

40. (Previously presented) The method as in Claim 39 further comprising means for recognizing biometric attributes of an individual.

41. (Currently amended) The system as in Claim 17, wherein said recipient data comprises, at least in part, a computer generated user code associated with said recipient ~~accessing~~ party.

42. (Previously presented) The method as in Claim 1,

wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

43. (Currently amended) The method as in Claim 1,

wherein said recipient computer is a user system that is directly accessible by said recipient ~~accessing~~ party, said user system including an electronic mail processing software and being capable of receiving e-mail.

44. (Currently amended) The method as in Claim 3,

wherein said recipient ~~accessing~~ party identity information is stored in the recipient computer.

45. (Previously presented) The method as in Claim 3,

wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

46. (Currently amended) The method as in Claim 4,
wherein said recipient ~~accessing~~ party identity information is stored in said computer.

47. (Previously presented) The method as in Claim 4,
wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

48. (Previously presented) The method as in Claim 4,
wherein said computer is the recipient computer.

49. (Previously presented) The method as in Claim 4,
wherein said computer is a remote user computer.

50. (Previously presented) The method as in Claim 1, wherein the discovering step includes electronically tapping the remote connection between the computer associated with the sending party and the recipient computer for obtaining remote access information associated with the remote connection.

51. (Previously presented) The method as in Claim 1, wherein said confirmation of receipt notice is used to verify proper delivery of legal documents.

52. (Previously presented) The method as in Claim 1, wherein said confirmation of receipt notice is used to verify proper delivery of confidential documents.

53. (Currently amended) The method as in Claim 1, wherein said recipient data comprises, at least in part, identity information associated with said recipient ~~accessing~~ party.

54. (Previously presented) The method as in Claim 53, wherein said identity information pertains to biometric identification.

55. (Previously presented) The method as in Claim 54 further comprising means for recognizing biometric attributes of an individual.

56. (Currently amended) The method as in Claim 1, wherein said recipient data comprises, at least in part, a computer generated user code associated with said recipient ~~accessing~~ party.

57. (Currently amended) A method of verifying whether an e-mail sent by a sending party was delivered to the intended recipient, said method comprising:

a) acquiring an e-mail for transmission to a target recipient;

b) transmitting said e-mail from a sender computer that is connected to the communications network;

c) delivering said e-mail to a recipient e-mail address, said recipient e-mail address associated with a recipient computer;

d) upon the occurrence of an access event, searching for recipient data from a target location associated with said recipient data, said recipient data associated with the recipient party;

e) generating a confirmation of receipt notice wherein the obtained recipient data is included in said confirmation of receipt notice;

f) transmitting said confirmation of receipt notice to an e-mail address associated with said sending party, wherein~~after~~, the obtained recipient data ~~on~~ contained in said confirmation of receipt notice can be compared to delivery ~~data~~ information associated with said intended recipient in order to verify if the e-mail was ~~properly~~ delivered to the intended recipient.

58. (Previously presented) The method as in Claim 57 further including the step of including in said confirmation of receipt notice access event data of attendant conditions of said access event

59. (Previously presented) The method as in Claim 57, wherein said target location is said recipient computer.

60. (Previously presented) The method as in Claim 57, wherein said target location is a remote user computer which is remotely connected to the recipient computer and from which the recipient party may gain remote access to the recipient e-mail address.

61. (Previously presented) The method as in Claim 57, wherein said target location comprises the remote connection between said recipient computer and a remote user computer, said remote connection being electronically tapped in order obtain said recipient data.

62. (Previously presented) The method as in Claim 57, wherein said target location comprises the remote connection between said sender computer and recipient computer, said remote connection being electronically tapped in order obtain said recipient data.

63. (Previously presented) The method as in Claim 57, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

64. (Previously presented) The method as in Claim 57, wherein said recipient computer is a user system that includes an electronic mail processing software and is capable of receiving e-mail.

65. (Previously presented) The method as in Claim 57, wherein the searching step includes retrieving a pre-recorded data file containing pre-recorded recipient data.

66. (Currently amended) The method as in Claim 57,

further comprising the steps of: obtaining recipient party identity information as a requisite condition for permitting access to the recipient email address ~~account or e-mail~~, said identity information configured to ~~precisely~~ identify said recipient party, and

wherein the step of obtaining recipient data from a target location associated with said recipient data includes retrieving the recipient party identity information.

67. (Previously presented) The method as in Claim 66,

wherein said recipient party identity information is stored in the recipient computer.

68. (Previously presented) The method as in Claim 66,

wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

69. (Currently amended) The method as in Claim 57, further comprising the steps of:

obtaining recipient party identity information as a requisite condition for operating a computer, and

wherein said identity information is configured to ~~precisely~~ identify said recipient party, and the step of obtaining recipient data from a target location associated with said recipient data includes retrieving the recipient party identity information.

70. (Previously presented) The method as in Claim 69,

wherein said recipient party identity information is stored in said computer.

71. (Previously presented) The method as in Claim 69,

wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

72. (Previously presented) The method as in Claim 69, wherein said computer is the

recipient computer.

73. (Previously presented) The method as in Claim 69, wherein said computer is a remote user computer.

74. (Previously presented) The method as in Claim 57, wherein said confirmation of receipt notice is used to verify proper delivery of legal documents.

75. (Previously presented) The method as in Claim 57, wherein said confirmation of receipt notice is used to verify proper delivery of confidential documents.

76. (Previously presented) The method as in Claim 57, wherein said recipient data comprises, at least in part, identity information associated with said recipient party.

77. (Previously presented) The method as in Claim 76, wherein said identity information pertains to biometric identification.

78. (Previously presented) The method as in Claim 77 further comprising means for recognizing biometric attributes of an individual.

79. (Previously presented) The method as in Claim 57, wherein said recipient data comprises, at least in part, a computer generated user code associated with said recipient party.

80. (Currently amended) A process for verifying whether e-mail sent by a sending party was delivered to the intended recipient, said process comprising:

a) acquiring an e-mail for transmission to a target recipient;

b) transmitting said e-mail from a sender computer that is connected to the communications network;

c) delivering said e-mail to a recipient e-mail address, said e-mail address associated with a recipient computer;

d) upon the occurrence of an access event, searching for recipient data that is associated with the recipient party;

e) generating a confirmation of receipt notice wherein the discovered recipient data is included in said confirmation of receipt notice;

f) transmitting said confirmation of receipt notice to an e-mail address associated with said sending party, whereinafter, the discovered recipient data contained in said confirmation of receipt notice can be compared to delivery ~~data~~ information associated with said intended recipient in order to verify if the e-mail was ~~properly~~ delivered to the intended recipient.

81. (Previously presented) The process of Claim 80, wherein the step of searching for recipient data is conducted by searching said recipient computer.

82. (Previously presented) The process of Claim 80, wherein the step of searching for recipient data is conducted by searching a remote user computer which is remotely connected to the recipient computer and from which the recipient party may gain remote access to the recipient e-mail address.

83. (Previously presented) The process of Claim 80, wherein the step of searching for recipient data is conducted by electronically tapping the remote connection between said recipient computer and a remote user computer.

84. (Previously presented) The process of Claim 80, wherein the step of searching for recipient data is conducted by electronically tapping the remote connection between said sender computer and said recipient computer.

85. (Previously presented) The process of Claim 80, wherein said recipient computer is a

server of a service provider that is capable of receiving e-mail.

86. (Previously presented) The process of Claim 80, wherein said recipient computer is a user system that includes an electronic mail processing software and is capable of receiving e-mail.

87. (Previously presented) The process of Claim 80, wherein the searching step includes retrieving a pre-recorded data file containing pre-recorded recipient data.

88. (Currently amended) The process of Claim 80,

further comprising the steps of: obtaining recipient party identity information as a requisite condition for permitting access to the recipient e-mail address ~~account or e-mail~~, said identity information configured to ~~precisely~~ identify said recipient party, and

wherein the step of searching for recipient data includes retrieving the recipient party identity information.

89. (Previously presented) The process of Claim 88,

wherein said recipient party identity information is stored in the recipient computer.

90. (Previously presented) The process of Claim 88,

wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

91. (Currently amended) The process of Claim 80,

further comprising the steps of:

obtaining recipient party identity information as a requisite condition for operating a computer, and

wherein said identity information is configured to ~~precisely~~ identify said recipient party, and the step of searching for recipient data includes retrieving the recipient party identity information.

92. (Previously presented) The process of Claim 91, wherein said recipient party identity information is stored in said computer.

93. (Previously presented) The process of Claim 91, wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

94. (Previously presented) The process of Claim 91, wherein said computer is the recipient computer.

95. (Previously presented) The process of Claim 91, wherein said computer is a remote user computer.

96. (Previously presented) The process of Claim 80, wherein said confirmation of receipt notice is used to verify proper delivery of legal documents.

97. (Previously presented) The process of Claim 80, wherein said confirmation of receipt notice is used to verify proper delivery of confidential documents.

98. (Previously presented) The process of Claim 80, wherein said recipient data comprises, at least in part, identity information associated with said recipient party.

99. (Previously presented) The process of Claim 98, wherein said identity information pertains to biometric identification.

100. (Previously presented) The process of Claim 99 further comprising means for recognizing biometric attributes of an individual.

101. (Previously presented) The process of Claim 80, wherein said recipient data comprises, at least in part, a computer generated user code associated with said recipient party.

102. (Currently amended) A system for verifying whether e-mail sent by a sending party was delivered to the intended recipient, said system comprising:

a) a sender computer connected to the communications network and from which an e-mail is transmitted;

b) a recipient computer connected to said communications network, said recipient computer being capable of receiving said transmitted e-mail and further having data storage means for storing said received e-mail;

c) software capable of detecting an access event, wherein upon detection of said access event, said software executes the following steps:

1) searching for recipient data associated with the recipient party;

2) including the discovered recipient data in a confirmation of receipt notice;

d) means for transmitting said confirmation of receipt notice to an e-mail address associated with said sending party, whereinafter, the data contained in said confirmation of receipt notice can be compared to delivery ~~data~~ information associated with said intended recipient in order to verify if the e-mail was ~~properly~~ delivered to the intended recipient.

103. (Previously presented) The system as in Claim 102, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

104. (Previously presented) The system as in Claim 102, wherein said recipient computer is a user system that is directly accessible by said recipient party, said user system including an electronic mail processing software and being capable of receiving e-mail.

105. (Previously presented) The system as in Claim 102, further comprising a remote user computer which is remotely connected to the recipient computer.

106. (Previously presented) The system as in Claim 102, further comprising a pre-recorded recipient data file containing the recipient data, and wherein the executable software means for searching operates to retrieve the pre-recorded recipient data file.

107. (Previously presented) The system as in Claim 102, wherein the executable software means for searching operates to search for remote access information associated with the remote access of the recipient e-mail address from the remote user computer.

108. (Currently amended) The system as in Claim 102, further comprising recipient party identifier means resident on the recipient computer for obtaining recipient party identification information as a requisite condition for permitting access to the ~~recipient~~ e-mail ~~account or email~~, said identity information configured to ~~precisely~~ identify said recipient party, and

wherein the executable software means for searching for recipient data operates to retrieve the recipient party identification information.

109. (Previously presented) The system as in Claim 108, wherein said recipient party identification information is stored in the recipient computer.

110. (Previously presented) The system as in Claim 108, wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

111. (Currently amended) The system as in Claim 102,

further comprising recipient party identifier means for obtaining recipient party identification information as a requisite condition for operating a computer, said identity information

configured to ~~precisely~~ identify said recipient party, and

wherein the executable software means for searching for recipient data operates to retrieve the recipient party identification information.

112. (Previously presented) The system as in Claim 111 wherein said recipient party identification information is stored in said computer.

113. (Previously presented) The system as in Claim 111 wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

114. (Previously presented) The system as in Claim 111, wherein said computer is the recipient computer.

115. (Previously presented) The system as in Claim 111, wherein said computer is a remote user computer.

116. (Previously presented) The system as in Claim 102, wherein the executable software means for searching for recipient data operates to electronically tap the remote connection between the recipient computer and the remote user computer for obtaining recipient data associated with the remote connection.

117. (Previously presented) The system as in Claim 102, wherein the executable software means for searching for recipient data operates to electronically tap the remote connection between the sender computer and recipient computer for obtaining recipient data associated with the remote connection.

118. (Previously presented) The system as in Claim 102, wherein said confirmation of receipt notice is used to verify proper delivery of legal documents.

119. (Previously presented) The system as in Claim 102, wherein said confirmation of receipt notice is used to verify proper delivery of confidential documents.

120. (Previously presented) The system as in Claim 102, wherein said recipient data comprises, at least in part, identity information associated with said recipient party.

121. (Previously presented) The system as in Claim 120, wherein said identity information pertains to biometric identification.

122. (Previously presented) The system as in Claim 121 further comprising means for recognizing biometric attributes of an individual.

123. (Previously presented) The system as in Claim 102, wherein said recipient data comprises, at least in part, a computer generated user code associated with said recipient party.

124. Currently amended) A method of verifying whether a legal document sent by a sending party was delivered to the intended recipient, said method comprising:

a) acquiring an e-mail comprising of at least one legal document for transmission to a target recipient;

b) transmitting said e-mail from a sender computer that is connected to the communications network;

c) delivering said e-mail to a recipient e-mail address, said e-mail address associated with a recipient computer;

d) upon the occurrence of an access event, searching for recipient data that is associated with the recipient party;

e) generating a confirmation of receipt notice wherein the discovered recipient data is included in said confirmation of receipt notice;

f) transmitting said confirmation of receipt notice to an e-mail address associated with said sending party, whereinafter, the recipient data contained in said confirmation of receipt notice can be compared to delivery ~~data~~ information associated with said intended recipient in order to verify if the e-mail was ~~properly~~ delivered to the intended recipient.

125. (Previously presented) The method as in Claim 124, wherein said at least one legal document is a complaint.

126. (Previously presented) The method as in Claim 124, wherein said at least one legal document is a summons.

127. (Previously presented) The method as in Claim 124, wherein said at least one legal document is a jury duty notice.

128. (Previously presented) The method as in Claim 124, wherein said at least one legal document is a subpoena.

129. (New) The method as in Claim 3 wherein said recipient party is the accessing party.

130. (New) The method as in Claim 4 wherein said recipient party is the accessing party.

131. (New) The method as in Claim 5 wherein said recipient party is the accessing party.

132. (New) The method as in Claim 43 wherein said recipient party is the accessing party.

133. (New) The method as in Claim 53 wherein said recipient party is the accessing party.

134. (New) The method as in Claim 56 wherein said recipient party is the accessing party.

135. (New) The system as in Claim 18 wherein said recipient party is the accessing party.

136. (New) The system as in Claim 19 wherein said recipient party is the accessing party.

137. (New) The system as in Claim 20 wherein said recipient party is the accessing party.

138. (New) The system as in Claim 21 wherein said recipient party is the accessing party.

139. (New) The system as in Claim 27 wherein said recipient party is the accessing party.

140. (New) The system as in Claim 38 wherein said recipient party is the accessing party.

141. (New) The system as in Claim 41 wherein said recipient party is the accessing party.

142. (New) A method for verifying whether e-mail sent by a sending party was delivered to the intended recipient, said method comprising:

a) acquiring an e-mail for transmission to a target recipient;

b) transmitting said e-mail from a sender computer that is connected to the communications network;

c) delivering said e-mail to a recipient e-mail address, said e-mail address associated with a recipient computer;

d) upon the occurrence of an access event, discovering recipient data that is associated with the recipient party;

e) generating a confirmation of receipt notice wherein the discovered recipient data is included in said confirmation of receipt notice;

f) sending said confirmation of receipt notice to said sending party, wherein, the discovered recipient data contained in said confirmation of receipt notice can be compared to delivery information associated with said intended recipient in order to verify if the e-mail was delivered to the intended recipient.

143. (New) The method as in claim 1,

further comprising the step of: obtaining recipient party identity information from the recipient party as a requisite condition for permitting access to the e-mail file, and

wherein the discovering step includes retrieving the recipient party identity information, and wherein the generating step includes such recipient party identity information within the data contained in the confirmation of receipt notice.

144. (New) The method as in Claim 143,

wherein said recipient party identity information is stored in the recipient computer.

145. (New) The method as in Claim 143,

wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

146. (New) The system as in claim 17,

further comprising recipient party identifier means for obtaining recipient party identification information from the recipient party as a requisite condition for permitting access to the e-mail file; and

wherein the second executable software means for discovering recipient data operates to retrieve the recipient party identification information.

147. (New) The system as in Claim 146,

wherein said recipient party identification information is stored in the recipient computer.

148. (New) The system as in Claim 146,

wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

149. (New) The method as in Claim 57,

further comprising the steps of: obtaining recipient party identity information as a requisite condition for permitting access to the email file, said identity information configured to identify said recipient party, and

wherein the step of obtaining recipient data from a target location associated with said recipient data includes retrieving the recipient party identity information.

150. (New) The method as in Claim 149,

wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

151. (New) The process of Claim 80,

further comprising the steps of: obtaining recipient party identity information as a requisite condition for permitting access to the e-mail, said identity information configured to identify said recipient party, and

wherein the step of searching for recipient data includes retrieving the recipient party identity information.

152. (New) The process as in Claim 151,

wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

153. (New) The system as in Claim 102, wherein an intended recipient email address is associated with the intended recipient, the system further comprising:

recipient party identifier means resident on the recipient computer for obtaining recipient party identification information as a requisite condition for permitting access to the intended recipient e-mail address, said identity information configured to identify said recipient party, and

wherein the executable software means for searching for recipient data operates to retrieve the recipient party identification information.

154. (New) The process as in Claim 153,

wherein said identity information pertains to biometric identification, password identification, a computer generated user code, or a combination thereof.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.